

SECURITY SERVICES

M(X)DR for Microsoft 365 Defender

THE DIGITAL WORLD HAS CHANGED.

New way of working

The modern workplace evolved to a mobile workforce who work and connect to company assets wherever and whenever they desire. To enable this, organizations are shifting their data, services and workloads to the cloud, which once more has forced companies to redefine the organization's perimeter.

Cybercrime getting more sophisticated

The rise in the sophistication of cyber threats require organizations to take additional steps. Not only has the volume and extent of these attacks increased, also the speed at which attacks unfold has gone up significantly. From initial access to lateral movement to exfiltration, attacks can happen in a very short length of time, leaving a relatively little window of opportunity for defenders to step in and take remediating actions.



Our solution

Cegeka provides a M(X)DR service using the Microsoft 365 Defender platform which covers the full lifecycle, from Prevent over Detect and Investigate to Respond. By this service we will protect your identities and ensure that your employees use applications in a secure way. We reduce the potential impact of an attack by monitoring and taken required actions in a 24x7 mode.

Key benefits

**Broad 24x7
Detection**

Gain a broad visibility of your environment which is 24x7 monitored to detect advanced threats

**Respond & recover
as far as needed**

Because every second counts, we take action to contain the threat with automated threat response according to what is desired.

**Resilience &
transparency**

Our Security Advisors provide guidance on improving your Security Posture. Combined with Horizon this will give a continuous view on how everything is evolving.



DETECTION

Advanced Threat Intel

Using Industry-leading threat intel to detect real-time threats in your environment

Threat hunting

Intel-based Threat hunting to detect attacks which bypassed your defenses

24x7 Security Monitoring

Our SOC analysts will 24x7 continuously monitoring the MS 365 Defender platform and perform investigations to uncover Security Incidents

RESPONSE

Threat response

Off the shelf response actions which we will take upon approval or fully automated

CSIRT Services

Provide assistance for digital forencics, compromise assess or red teaming assessments.

RESILIENCE & RECOVERY

Service management

Monthly security service meetings to see what has happened and what the evolution is.

Security Advisory

Our security advisor will provide actionable resilience improvement to strengthen the security posture.

Technology Experts

In-house experts who can assisted in recovering impacted infrastructure and workplace.

Why use Microsoft 365 Defender?

- Powered by Cloud-native technology
- Best-of-class threat investigation and Response tools
- Broad attack surface coverage for endpoints, identities, office365 and data.
- Built-in security posture management through Secure Score
- Industry recognitions: Forrester Wave, Gartner Magic Quadrants



Why combine Cegeka & Microsoft 365 Defender

We help you with:

- **Set up and configure** Microsoft Defender solutions to protect endpoints, applications, identities, and office 365.
- **24x7 Managed Detection & Response** service across Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, Defender for Office and Azure AD Identity Protection.
- **Actual Threat Response** to contain Security Incidents
- Working with **Certified Microsoft experts**
- **Monthly Security meetings** to improve resilience
- **End-to-end Security response services**, fully integrated with other infrastructure solutions.

